Information Disclosure and Denial-of-Service Vulnerability in Multiple Air Conditioning Systems

Release date: July 1, 2021
Mitsubishi Electric Corporation

■Overview

Mitsubishi Electric air conditioning systems have an information disclosure and Denial-of-Service (DoS) vulnerability due to improper restriction of XML external entity reference (XXE) (CWE-611). A malicious attacker may disclose some of data in the air conditioning system or cause DoS condition by sending a specially crafted packet (CVE-2021-20595).

■CVSS

CVE-2021-20595 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:H Base Score:9.3

■Affected products

<Models and Versions>

【Air Conditioning System / Centralized Controllers】

Model	Versions
G-50A	Ver.3.35 and prior
GB-50A	Ver.3.35 and prior
GB-24A	Ver.9.11 and prior
AG-150A-A	Ver.3.20 and prior
GB-50ADA-A	Ver.3.20 and prior
EB-50GU-A	Ver 7.09 and prior
AE-200A	Ver 7.93 and prior
AE-50A	Ver 7.93 and prior
EW-50A	Ver 7.93 and prior
TE-200A	Ver 7.93 and prior
TE-50A	Ver 7.93 and prior
TW-50A	Ver 7.93 and prior

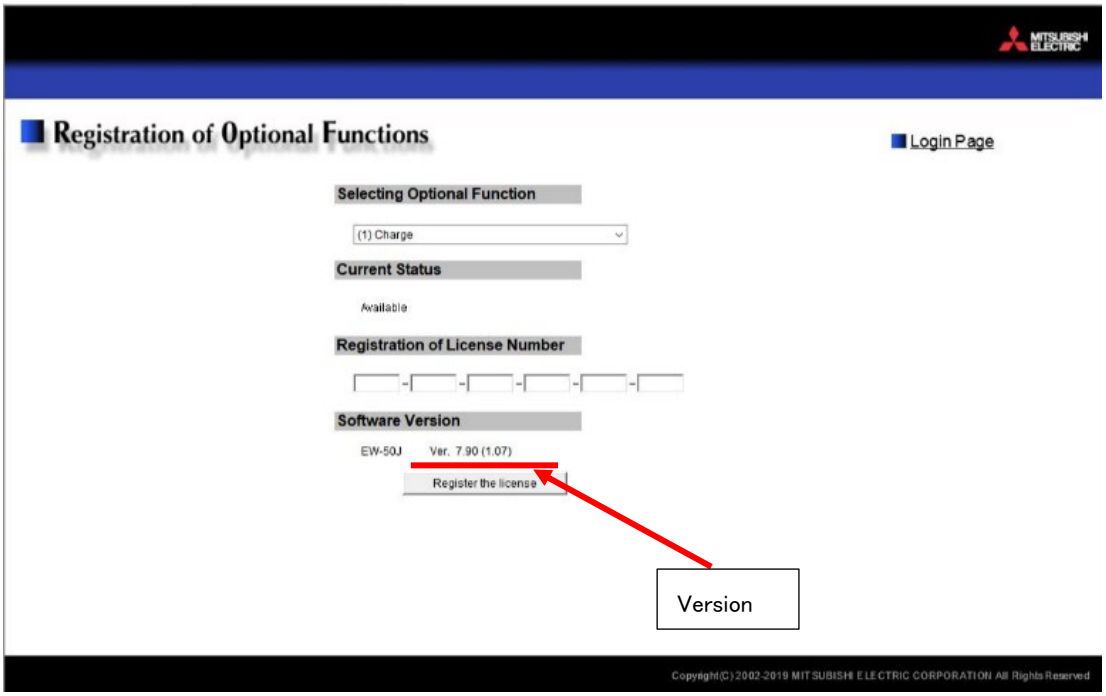
【Air Conditioning System /BM adapter】

Model	Versions
BAC-HD150	Ver.2.21 and prior

<How to check the versions>

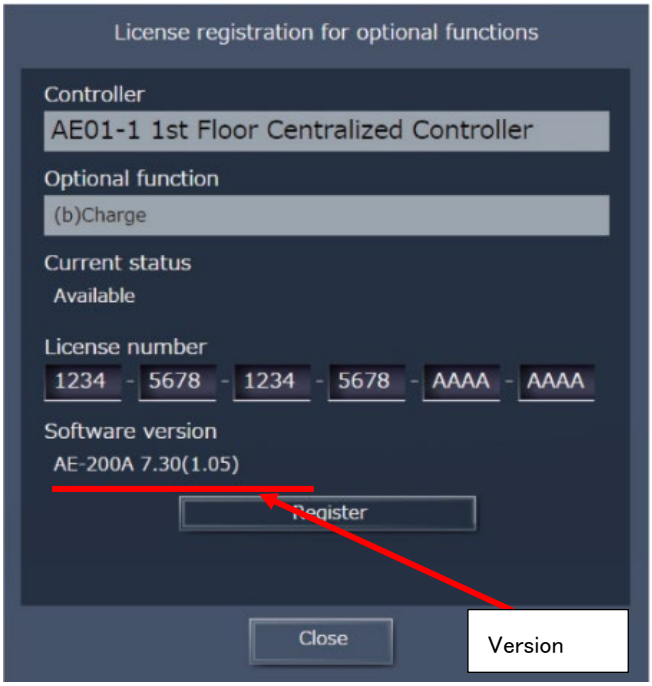
・G-50A、GB-50A, GB-24A, AG-150A-A, GB-50ADA-A, and EB-50GU-A.

By selecting [Registration of Optional Functions] on Login Page of their WEB screen, you can check the versions.



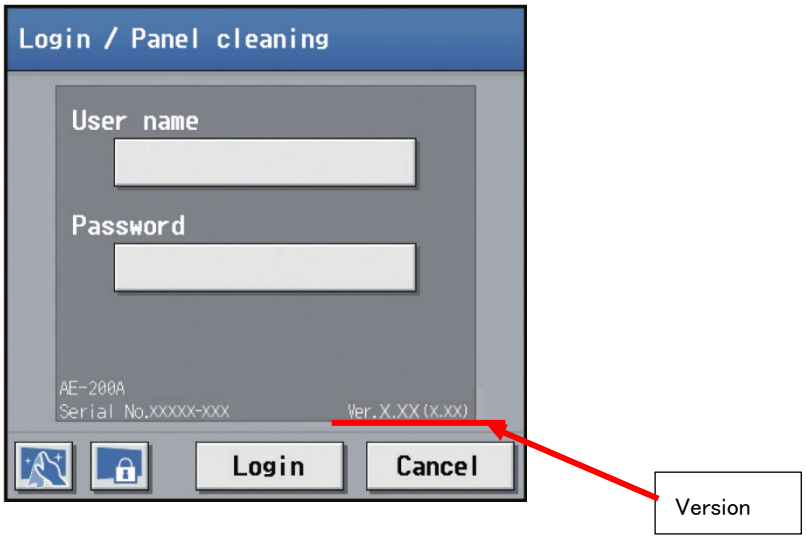
・AE-200A, AE-50A, EW-50A, TE-200A, TE-50A, and TW-50A

By selecting [License Registration] on Setting tab of the home screens after you log in as administrators on their WEB screen, you can check the versions.



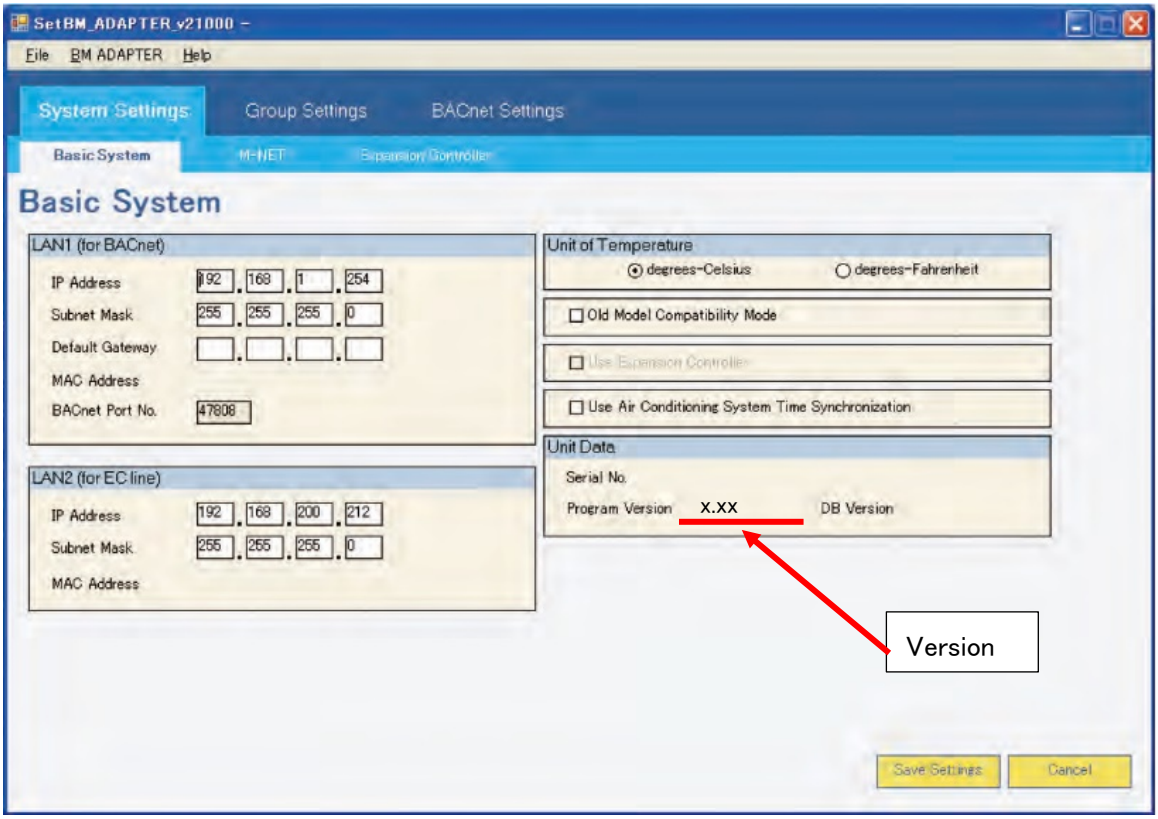
・Another way to check versions of AG-150A-A, AE-200A, AE-50A, TE-200A, and TE-50A

By touching on the upper right corner of the normal screens to display the login window, you can check the versions.



・BAC-HD150

By clicking [Get Settings] on Basic System window of the Setting Tool, you can check the version.



■Description

Mitsubishi Electric air conditioning systems have an information disclosure and DoS vulnerability due to improper restriction of XML external entity reference (XXE) (CWE-611).

■Impact

A malicious attacker may access the data in the air conditioning system or cause DoS condition by sending a specially crafted packet.

■Countermeasures

The following models are unaffected if they are running the software firmware versions (or later) as indicated below.

<Models and Versions>

【Air Conditioning System / Centralized Controllers】

Model	Versions
G-50A	Ver.3.37 or later
GB-50A	Ver.3.37 or later
GB-24A	Ver.9.12 or later
AG-150A-A	Ver.3.21 or later
GB-50ADA-A	Ver.3.21 or later
EB-50GU-A	Ver 7.10 or later
AE-200A	Ver 7.95 or later
AE-50A	Ver 7.95 or later
EW-50A	Ver 7.95 or later
TE-200A	Ver 7.95 or later
TE-50A	Ver 7.95 or later
TW-50A	Ver 7.95 or later

【Air Conditioning System /BM adapter】

Model	Versions
BAC-HD150	Ver.2.22 or later

<How to update>

Please contact your distributor or a Mitsubishi Electric representative. The updated software is available on MyLinkDrive.com.

■Mitigations

1. Update the software firmware as soon as possible.
2. Mitsubishi Electric recommends the following mitigation measures as noted in our equipment manuals to minimize the risk of exploiting this vulnerability,
    a. Use a VPN router, etc. when you connect your air conditioning system to the Internet.
    b. Use anti-virus software on your computer to connect your air conditioning system.
    c. Restrict access to your air conditioning system from untrusted networks and hosts.
    d. Change default user names and passwords.

■Acknowledgement

Mitsubishi Electric would like to thank Howard McGreehan of Aon's Cyber Solutions who reported this vulnerability.

■Contact information

Please contact your local Mitsubishi Electric representative.